金融行业安全指导

金融行业安全指导

安全是金融行业永远的话题。现在网络犯罪分子们越来越多的利用综合渠道，包括网络，手机，邮件等，制造机会，跟踪欺诈消费者。

金融行业面临的安全风险和挑战有哪些？有什么方法和措施可以增强金融行业安全性？用户身份如何管理？用户数据如何防泄密？

本技术手册将从三个方面为您提供详细的安全策略，包括：金融安全风险及挑战，案例学习：金融安全启示录和金融安全最佳实践。

金融安全风险及挑战

随着金融行业的不断发展，金融管理全面实现了电子化，服务品种不断增加，网上银行、电话银行、网上证券、网上保险、移动炒股等产品不断涌现。但是，多样化业务在给客户带来方便的同时，,金融行业的风险也呈现出复杂多变的特征。无论是敏感信息泄漏还是个人身份泄漏，金融行业都位居前列。

金融安全面临哪些挑战？行业内部又是如何看待这些挑战的呢？

- ❖RSA：多服务渠道金融犯罪
- ❖网银欺诈成为银行业务流失的罪魁
- ❖移动支付的应用风险
- ❖调查显示：金融业将增加安全支出

案例学习：金融安全启示录

在银行与窃贼们的技术抗衡过程中，金融机构一直在强化他们的网络安全措施以防止骗子们的新的攻击。花旗银行 ATM 机网络被黑以及由此带来的信用卡持卡人帐号和身份认证信息的暴露，给金融机构带来了新的安全忧虑并促使这些机构重新审视他们的安全方案。

- ❖从花旗银行 ATM 机被黑中汲取教训
- ❖LendingTree 事件启示录（上）
- ❖LendingTree 事件启示录（下）

金融安全最佳实践

金融行业的风险防范大多是跟技术和运营层面相关，而风险防范最大的核心部分就是信息安全。如何控制风险、确保“安全”已成为金融行业面临的重大课题。

- ❖身份管理联盟最佳实践（上）
- ❖身份管理联盟最佳实践（下）
- ❖鉴定网银用户身份的最佳程序
- ❖网上银行安全的评估工具
- ❖如何检测和预防内部欺诈？
- ❖金融服务领域数据分类的最佳实践
- ❖如何阻止 ATM 卡片浏览诈骗
- ❖数据屏蔽最佳实践的四大要素

RSA：多服务渠道金融犯罪

罪犯正在利用综合渠道，包括网络，手机，邮件等，制造机会，跟踪欺诈消费者。金融服务行政人员在 4 月 10 的 2008 RSA 大会讨论时如此说。

"这只是一个小小的打地鼠游戏。" Bank of the West 银行的副总 Lan McGowan 说。

在某些情况下，罪犯会收集在线消费者信息，并利用这些信息通过电话进行银行业务处理。

另外，骗子会给呼叫中心打电话，并利用社会工程重设用户认证，然后再联机，参与讨论的人说。Discover Financial Services 的网络欺诈和企业安全经理，Cynthia Bohman 说，罪犯都是机会主义者，他们利用任何可以发动攻击的渠道。她说，有时，看似微小的业务处理，比如通过电话进行的地址变更，就可能使一次大型欺诈的一部分

Bohman 说她的公司的呼叫中心使用共享的秘密提问，并且根据与业务处理相关的风险等级的不同，而增加问题。但是仍然不选择使用带外认证，就是通过另外一种方式和消费者联系确认业务，应为调查显示，消费者不想要这么做。

E*Trade Financial 公司的安全架构经理，Andy Wen 说，认证密码给消费者提供了他们希望的可视性安全。"如果你服务于一家金融机构，就需要研究适合用户基础的是什么。"他补充说公司着眼于新型的安全认证。

McGowan 说他的公司将要在警惕高风险的用户业务处理时，在银行的在线系统上增加正文信息。他说："我们正在从更广的角度审视我们的安全策略。"

讨论小组的成员说，他们正在研究移动银行等新渠道带来的风险。尽管如此，McGowan 注意到，处理起来实际非常简单，"新渠道的安全问题处理起来比较简单……，而挑战又回到传统渠道和传统渠道的翻新上面了。"

对于未来，参加讨论的人员说，他们没有看到利用多渠道的骗子将会马上转变方向。

Wen 说"我发现这个问题越来越复杂，因为我们想要从多方面为消费者提供服务……，也就意味着，攻击的层面变得更大了。"

(作者：Marcia Savage　译者：Tina Guo　来源：TechTarget 中国)

网银欺诈成为银行业务流失的罪魁

根据调查显示，许多经受过网上银行欺诈或者其他欺诈遭遇的企业银行顾客倾向于更换银行。

根据一项针对美国中小企业的 533 名雇员的调查，40%遭受过欺诈的企业将他们部分或者全部的企业银行账户转移到其他银行。这其中 11%的企业与他们的银行彻底终结关系，29%的企业则将他们的主要账户转移至其他银行。

总部位于加州洛斯阿多斯的防止在线欺诈公司 Guardian Analytics 受 Ponemon Institute 的委托进行了这项调查。该公司的总裁兼 CEO 特里.奥斯丁表示，“当企业遭受欺诈或者未遂欺诈袭击后，他们倾向于以此为转折点，而决定是否继续留在这个银行。”

在《2010 年企业银行信用调查》中指出有超过一半（55%）的受访者在去年经历过欺诈攻击，其中 58%是在线攻击行为。

联邦政府官员们发出警告称去年针对中小企业的在线企业银行账户的攻击激增。FBI 估计针对中小企业的 ACH 欺诈案造成了大约 1 亿美元的损失。

根据调查，在 80%的欺诈案例中，银行未能在交易之前发现欺诈活动，同时有 87%的案例显示银行没能完全恢复被盗资产。57%的被调查者表示他们的损失没有得到完全赔偿。

67%的受访者表示他们的银行应该为保护他们的账户负最终责任，但只有 30%的人表示他们的银行具有很强的安全性。

“银行有很多机会可以做得更好”，奥斯汀说。

他表示，银行可以采取的方式是与他们的企业银行客户就安全策略问题进行更有效地沟通。24%的受访者认为他们的银行没有就保护企业账户免受欺诈的政策进行解释。

Hillary Machinery 公司是一家位于特科萨斯州 Plano、拥有 20 名员工的小企业。在去年下半年该公司遭受了在线银行欺诈，公司销售与市场副总裁特洛伊欧文表示，他们正在将其账户转移至另一家银行。在遭受网络攻击后，Hillary Machinery 公司被他的前银行、总部位于达拉斯的 PlainsCapital 银行起诉。这个极不寻常的案件最初由新闻记者 Brian Krebs 在他的博客中报道出来。

上个月，该公司以遭受网络抢劫为由反诉 PlainsCapital 银行，称犯罪分子从 Hillary Machinery 公司的一个商业户头上窃取了 80 多万美元，而银行方面追回了近 60 万美元。

“我们是一家十分健康的公司，这个事件没有打垮我们”，欧文针对这笔欺诈损失表示，“但是这迫使我们推迟了一些合作计划。”

他表示，安全是寻找下一个新银行的首要考虑因素。“在这一点上，我们深知要问什么问题”，他补充道。

大部分小企业都没有意识到针对消费者的在线银行保护策略并不适用于企业银行客户，欧文表示，“他们以为一旦当你将钱存入银行，它们就安全了”。

（作者：Marcia Savage　译者：叶蓬　来源：TechTarget 中国）

移动支付的应用风险

移动付款被吹捧为最简单的、最方便的资金交换方式，通过移动付款几乎在任何地方都能以电子支付的方式进行购物和支付账单。用户只需单击一下移动设备的按钮或者在销售网点系统附近晃动一下移动设备，就可以进行购物或者支付账单。这对于购买者来说，支付和购物方便了很多；但是它却给提供这个服务的金融机构引入了很大的风险。

这不是移动银行业务第一次亮相了。几年前，在向电子货币和数字身份证转变的第二个革命性阶段就出现了移动付款的身影。那时移动付款业务的发展受到技术限制和高成本的困扰，不论是消费者还是服务提供商都面临这些方面的问题。无线应用协议（WAP1.0）的普及遭遇了很大的挫折，因为移动设备和移动业务服务提供商之间存在着巨大安全缺口，这一情况被叫做"WAP 缺口"。

今天，很多过去的技术限制和安全顾虑都已降低了，而移动付款业务利用这些技术上的进步又一次浮出了水面。其中一个重要的变化是 WAP 2.0 的使用，它允许在移动设备和服务提供商之间进行端到端的加密。

但是移动付款业务还是存在风险，金融机构采用移动付款程序之前，他们应该考虑以下几个关键的风险区域：

第三方供应商：移动付款服务提供商建立了一个机制，可以让用户把他们存在银行帐户或其它受监管的金融企业中的货币取出来。这些服务提供商是财务中间人，他们提供的服务被列为货币服务业务（MSBs）。货币服务业务提供商必须遵守与其合作的州内的法律。然而，不是所有的州都有监管 MSB 活动的法律，所以在选择的过程中应该仔细审查。如果你所在的财务公司决定使用 MSB 进行移动付款交易活动，那么请务必检查 MSB 提供商实际的信息安全情况，从而让自己放心。

监管和法律责任：美国现在几乎没有能够防止移动付款业务被滥用的安全措施。安全措施的规划和宣传指导方面几乎没有进步，传统的洗钱对策不能充分地处理因移动付款滥用引发的电子银行和无现金服务系统威胁。到现在为止，几乎没有任何基金会去研究和发展法律，从而执行现有的几个监管规则。金融机构必须让他们的法律团队和规则遵从团队制定使用移动付款系统的"交通规则（rules of the road）"。规则应该包括全面的 MSB 服务提供商实际安全情况审查，全面的支付卡行业数据安全标准(PCI DSS)的遵守情况审查，以及制定一个强有力的

涵盖突发事件应对和责任的合同。另外，如果一个金融机构参加了政治活动团体，则一定要教育和告知团体的代表们，让他们清楚为客户开发相关法律和安全措施的必要性。

预防欺诈/损失的措施：金融机构必须能够监视和跟踪可疑的交易活动，这就要求交易活动对金融机构是透明的，以便于其收集情报。这有时候需要得到政府情报机关和政府执法机构的协助。不幸的是，这些组织在移动付款技术方面几乎没有专业的技能。很多国家在通过移动电话进行货币转移领域没有相关的法律和监管政策。移动电话网络有一些安全功能，可以阻止执法部门和情报服务部门检测可疑的非法交易。迅速发展的技术能力正超过政府追踪货币交易的能力，甚至会使金融机构不必再遵守美国爱国者法案（USA Patriot Act）和银行保密法（Bank Secrecy Act）。

由于无线环境中安全威胁的属性和数量的不确定性，金融机构应该对他们的移动付款系统实行独立的、阶段性的安全漏洞评估，评估的重点放在那些能够识别可疑交易活动或者可疑付款活动的检测系统和反馈系统，这项工作非常的关键。另外，金融机构必须命令他们的第三方付款服务提供商也要进行评估，以便于他们进行审查。这些评估应该在每一次大的环境条件改变时进行。移动付款欺诈处理程序应该有利于对检测到的威胁和滥用展开迅速调查以解除威胁。这将帮助执法部门和政府情报机构在必要的情况下对你的企业进行协助。

总体而言，虽然移动付款业务在电子付款的可行性和安全方面已经有了一些显著的改进，但对于金融机构来说，现在采用这个服务还是有几个大的风险。随着培训和安全措施的改进，以及技术在市场上变得司空见惯，一定会浮现出新的风险和威胁来挑战今天的安全改进。移动付款可以更快、更方便、障碍更少，但是这些对于攻击者来说也是如此。金融机构必须权衡风险和利益，然后决定现在时机是否适当，能否出手一搏。

（作者：Rick Lawhorn　译者：Sean　来源：TechTarget 中国）

调查显示：金融业将增加安全支出

Independent Community Bankers of America (ICBA)的调查显示：保护客户数据是金融业首先关注的顶级技术，很多银行都计划增加安全技术方面的费用。

在本月上旬发布的 2008 ICBA Community Bank Technology Survey 中，1280 位回应者的 81%说保证客户数据的安全是他们最紧迫的问题。57%的人说他们计划在以后的两年中增加安全技术的支出，而 51%说他们将要增加在欺骗检测技术方面的支出。

ICBA 的支付和技术策略助理董事 Cary Whaley 说："在金融业层面，客户关系极为重要，所以保护客户数据时第一要务。"

这次调查是在六月进行的。调查还显示他们中的 81%都把身份窃取列为数据安全的首要关注点。63%的人说他们最担忧的是病毒攻击，而 61 的人则把黑客攻击列为首要威胁。

对内部威胁的态度存在有趣的分歧：资产超过一亿的银行中的 41%说内部威胁是首要安全关注点，而资产超过五亿的银行中有 68%。另外，小型银行相对于大型银行来说更关注外部黑客攻击（63%对 47% ）

Whaley 说："关键原因是（在小型银行中）没有很多的员工，对员工的了解也更深入。不但可以在工作的时候看到他们，在下班后和周日教堂中都可以看到他们。"

他说，这个协会每两年做一次技术调查，而数据安全一直在金融业的关注项目中居于高位，而今年的调查更加的细致。

和 2006 年的调查相对，入侵检测和防御（IDS/IPS）安全技术在金融业的采用有很大的提升。两年前，38%的银行采用了 IDS，而 25%采用了 IPS。今年，这些数字增加到了 80%和 73%。

Whaley 说他不觉得目前的经济形势会改变银行对安全关注和支出费用计划。

（作者：Marcia Savage　译者：Tina Guo　来源：TechTarget 中国）

从花旗银行 ATM 机被黑中汲取教训

花旗银行 ATM 机网络被黑以及由此带来的信用卡持卡人帐号和身份认证信息的暴露，给金融机构带来了新的安全忧虑并促使这些机构重新审视他们的安全方案。

在银行与窃贼们的技术抗衡过程中，金融机构一直在强化他们的网络安全措施以防止骗子们的新的攻击。

"那些家伙试图以诈骗的方式营生，而我们的使命就是阻止这一行为的发生"Doug Johnson 如是说。他是美国银行家协会风险管理政策部门的副主席。

花旗银行的案例

2008 年 2 月 1 日，花旗银行向美国联邦调查局报告说用户的帐号和身份认证信息被窃取了，这部分信息来源于 7－Eleven 便利店的处理交易的花旗银行自动柜员机服务器。根据联邦调查局的说法，被羁押的犯罪嫌疑人利用偷窃来的帐号编码制造了的新的 ATM 卡，从 ATM 机上面取出了现金。另外法庭的案卷显示这些被告人通过各种 ATM 机骗术窃取了多达 360 万美元现金。

微软效应

专家说，花旗银行的帐号被攻击的原因与微软操作系统遭受攻击的原因遵循相同的逻辑－－他们都无处不在。花旗银行是一家全球范围的金融服务企业，拥有广泛的 IT 基础设施和进 2 万的自动取款机；而微软的 Windows 操作系统运行在全世界超过 90%的个人电脑以及 70%的服务器上。越来越多的 ATM 网络运行在微软的 Windows 操作系统上，安全专家说如此一来会使得这些 ATM 网络比运行在专有的平台上更加脆弱，让黑客更容易得逞。可是，无论是花旗银行还是微软都不会透露花旗银行的 ATM 机网络是否是基于 Windows 操作系统的。

"作为黑客，如果你将花旗银行网络作为攻击目标来投入精力，你可以收获更多，因为在这个网络上你有更多的攻击机会，就像在 Windows 系统上一样。" Avivah Litan 说道。他是位于斯坦福康恩的 Gartner 公司的一名分析师。

虽然花旗银行没有确认运营公司，但是有两家公司负责维护这个 7-Eleven 便利店的 ATM 机：一家是位于休斯敦的在 seven-eleven 拥有 5500 台 ATM 机的 Cardtronics 公

司，另一家是布鲁克菲尔德威斯的 Fiserve 公司。Cardtronics 公司仅仅维护他的 5500 台 ATM 机中的 2000 台。而 Fiserv 公司负责维护剩余的 3500 台。根据美国证券交易委员会的备案记录，公开上市的 Cardtronics 公司在 2007 年末收购了 7－Eleven 的金融服务部。该服务部门是这家连锁便利店的一个分支机构。

Fiserv 通过一位发言人透露他们的服务器在花旗银行事件中没有被攻击。而 Cardtronics 公司拒绝对此作出评论。在 7 月 2 日发布的新闻中写道："Cardtronics 公司没有卷入这起犯罪指控之中，因此该公司预计也不会就这起案件发表任何陈述。"

支付卡行业标准不等于安全

但是 Cardtronics 公司补充说它的 ATM 机都有加密密码键盘，使用了三重数据加密，并且他们的处理平台是遵循支付卡行业数据安全标准的。

可是，遵循行业标准并不意味着一个 ATM 网络对黑客具有免疫性。Mike Urban 说："你不能说'我是遵循支付卡行业标准的'，然后你就可以高枕无忧了。这需要一种持久的安全意识，而且应该一直是一种持久的安全意识。"Mike 是 Fair Isaac 公司的防欺诈解决方案的高级主管，该公司是明尼阿波利斯的决策管理自动化服务提供商。

太多的网络管理员在部署网络的时候仅仅是为了达到支付卡行业标准，而这个标准却又是一直在改变的，Jim Pflaging 说道。他是位于旧金山市 SenSage 公司的 CEO，该公司是一家数据仓储工具提供商。

以前，一些公司仅仅达到了最低的安全标准。"他们只希望支付卡行业标准审计员尽快离开他们的办公室。" Jim 说。然而渐渐地，另外一些公司开始把网络安全问题看作是对他们的业务具有战略意义的风险管理的一种形式，并开始以超越 PCI 的标准严格要求自己。

ATM 安全演化

最近，ATM 机供应商与安全专业公司聚集在一起讨论开发新的技术以应付日益进化的黑客攻击。比如，Wincor Nixdorf，一家德国 ATM 机制造商，正在与思科系统公司一起开发 PC / E 平台安全代理。这种技术可以防止软件在没有被授权的情况在被安装或者修改。花旗银行案件背后的教训是，黑客在服务器上安装了恶意软件，用以访问服务器上的账号和密码信息。

另一对类似的合作伙伴是 Deibold 公司与 Agilis 软件有限责任公司。他们准备给 Deibold 的 Opteva ATM 机装备反盗读技术。盗读是指使用一个假冒的 ATM 卡槽代替真正的卡槽来读取插入到这个假冒的卡槽里的信用卡上面的帐号和密码信息。

但是，SenSage 的 Pflaging 分析说，这些孤立的产品并不能提供一个广泛的安全网络。然而，能够记录发生在网络上的每一个事件的数据仓储技术可以用来帮助识别可能的潜在窃取信息行为导致的网络事件之间的内在联系或者特征。比如，如果一个 ATM 机卡在芝加哥被使用了，不一会功夫，又一次在莫斯科被使用，那就是一个可疑的标志，Pfalging 如是说。如果一个银行的雇员访问了他们的内部网络，并且很快从网络上下载了一个很大的文件，那么他的行为需要被严格审查。

考虑到在花旗银行的案例中存在着花旗银行内部人员协助犯罪的可能，Pflaging 说，“这就好像给了你一双火眼金睛，使得你可以觉察到所有的这些非同寻常的举动，或者监视那些不知何故取得了你的信赖的内部人员凭证的人。”

虽然基于 Windows 的 ATM 网络存在很多安全漏洞，但是这种网络在金融机构中却被普遍应用。据 Pflaging 分析，Windows 之所以成为首选是因为它成本低并且它使得银行容易进行管理，特别是那些有跨国的全球网络的银行更是如此。“但是，对于安全方面的黑客来说，Windows 好比就是一封公开的邀请信。”

虽然 Windows 树大招风，但是它可以变得安全，Gartner 的 Litan 说。“如果你保持你的 Windows 系统的锁定状态并且也锁定你的网络，那么它就不会比任何其他系统差或者好。然而如何实现在锁定并且不让任何其他人登录进来的情况下工作呢？”

（作者：Robert Mullins　译者：行久　来源：TechTarget 中国）

LendingTree 事件启示录（上）

在客户数据被盗的入侵事件之后，LendingTree 的广告词"当银行开始竞争，你将受益"就成了笑柄。

在 Consumerist 网站（一个消费者权益保护网站）上的一条留言说“当银行被攻破，你将受害”。

事件

2008 年 4 月 21 日，LendingTree 公司被迫承认，它的前任在线抵押贷款代理雇员获取了用户的密码，并将其提供给未经 LendingTree 批准的其它抵押贷款提供者，以便他们向这些用户宣传他们自己的贷款产品。尽管公司向加州州立法院起诉了参与此次入侵的各方，还是有多个 LendingTree 的用户在联邦法庭上对 LendingTree 疏于网络安全提起了诉讼。

2008 年 4 月 21 日，LendingTree 公司被迫承认，它的前任在线抵押贷款代理雇员获取了用户的密码，并将其提供给未经 LendingTree 批准的其它抵押贷款提供者，以便他们向这些用户宣传他们自己的贷款产品。尽管公司向加州州立法院起诉了参与此次入侵的各方，还是有多个 LendingTree 的用户在联邦法庭上对 LendingTree 疏于网络安全提起了诉讼。

"我们对引起的所有不便表示歉意，"4 月 21 日一封发给客户的署名"RL Harris"的信件说道，这个署名明显来自 LendingTree 的主席 Robert L. Harris。Harris 指出前雇员将客户密码提供给了未经批准的放贷者，通过这种权限，未经批准的放贷者可以查看客户的抵押贷款申请表格。他还指出未经批准的访问最早从 2006 年 10 月开始。

他表示："贷款需要填写包括名字、地址、Email 地址、电话、社保号码、收入和受雇信息的表格。"尽管这些信息对身份盗窃者来说可能是一个宝库，Harris 还是试图消除客户的疑虑，说道："我们相信这次事件中没有发生任何的身份盗窃和财务欺诈行为。"LendingTree 的官方发言人拒绝对此发表评论。

在入侵被发现的时候，北卡罗来纳州 Charlotte 的 LendingTree 是 IAC/InterActiveCorp 的一个分支机构。它于 8 月 21 日脱离母公司成为独立上市公司 Tree.Com Inc。

在发现入侵的同时，LendingTree 起草了诉状状告 5 家南加利福尼亚州的抵押贷款放贷者，在诉状中指控他们未经授权使用他们的客户记录而涉嫌欺诈。这些公司是 Newport Lending Corp.、Southern California Marketing、Sage Credit Co.、Chapman Capital Inc.、 和 Home Loan Consultants。

后果

LedingTree 在加州的案件中作为原告的同时，也在多宗由 LendingTree 客户向联邦法庭提交的诉讼中作为被告，那些客户由于自己的记录被泄露而被激怒。

这些诉讼中的一个，纽约城的客户 Marvin Garcia，于 7 月 29 日在曼哈顿的美国地方法院状告 LendingTree，指责他们的疏忽、对隐私的侵害，以及对《美国公平信用报告法》的违反，其中要求公司"具备合理的规章以保证客户报告的使用的合法性。"

这一诉讼后来被与北卡罗来纳州（LendingTree 所在地）的其它客户诉讼合并，其中还提到了 LendingTree 在加利福尼亚所起诉的未经授权的放贷者"这些放贷者使用 LendingTree 客户的密码访问...客户的贷款申请表格来向他们推销贷款。"该诉讼指出："LendingTree 知道或者应该知道他们用来处理和保存客户贷款申请表格的网络...具有安全漏洞。"

在宣布递交 Garcia 诉状的时候，它的律师所，纽约 White Plains 的 Meiselman Denlea 指责 LendingTree 在发现入侵之后等待了太长的时间才警告他们的客户，而且仅仅是提醒客户检查信用记录并持续留意他们的信用报告——是他们自掏腰包。

(作者：Robert Mullins　译者：李博文　来源：TechTarget 中国)

LendingTree 事件启示录（下）

声誉风险不能忽略

可以预见 LendingTree 不管是在真正的法庭还是民意"法庭"上都会受到指责，Financial Insights（IDC 的一个专注于财务服务产业的研究公司）的全球风险管理研究主任 Dana Wiklund 说道。

"这给 LendingTree 带来声誉上的风险，"Wiklund 说道。不过，他补充说，这个入侵本可能会严重得多。截至目前，还没有证据表明这次对用户记录的未经授权的访问造成任何这些用户的身份被窃，或者针对这些客户的欺诈行为（尽管客户的诉状指出他们仍处在危险之中）。另外由于不知道到底有多少 LendingTree 的用户记录被暴露，他不认为这次事件像以往的入侵事件一样严重。

Wiklund 说："事实是，这些数据落到了其它的抵押贷款代理或者宣传人员的手中，这和丢失一盘写有上百万社会保险号码的磁带并发现其中的一些号码出现在国际诈骗团伙中是有天壤之别的。"他补充道，那些拿到了未经授权的访问权限的贷款代理或者放贷者大多是一两个人的小公司，他们的主要意图是想要增加自己的业务。

不管怎样，他总结道，LendingTree 必须要回过头去，看看到底是哪里出了问题并将其纠正。

密码保护

LendingTree 的雇员可以获取客户密码并将他们提供给外人，这使得 Jeremy Duffy 感到很迷惑，他自称为技术隐私意识的倡导者，并主持一个在线的讨论会"服务大众的计算机和因特网安全"。Duffy 很难相信公司的雇员可以访问哪怕他们自己的用户的密码。

需要确认的是密码是否被加密了。如果它们被加密过了，Duffy 说，"那就几乎不可能有什么人能知道确切的密码内容，就算他们有直接访问数据库的能力也无济于事。"如果它们没有加密，而是以明文保存。"那就造成所有能够访问数据库的人都能看到客户的密码，这是个严重的安全问题。"

Duffy 建议做一个简单的实验。如果一个用户在登录页面点击了那个"丢失密码"按钮，网站就给他们发送一封带有他们设置的密码的 email，那么密码多半是以明文存储的。如果它发回的是一个随机生成的密码，允许用户登入并重新设置密码，那它就可能是加了密的。

LendingTree 在公司网站上登出的隐私政策说公司使用"知名并审核过的安全技术。"用户输入个人信息的网页是通过 HTTPS 传送到客户的浏览器的，这是一种安全的服务器通信协议。浏览器和 LendingTree 的服务器之间的传输使用 SSL（Secure Sockets Layer ——安全套接字层）技术进行加密。

不过隐私政策的开始有一句很有深意的警告："无法保证在 Internet 上的数据传输或者信息存储技术是 100%安全的。"

（作者：Robert Mullins　译者：李博文　来源：TechTarget 中国）

身份管理联盟最佳实践（上）

人不是生活在真空之中，公司也不应该这样。为了在当今的市场上取得成功，金融公司不得不重新思考他们的商业运作模式。对传统实体金融公司而言，他们已经意识到利用所有的人事、系统和服务资源为公司内部的信息服务这种策略已经过时，游戏规则已经开始改变了。为了维持高效率、低成本的商业运作，他们不得不开始寻找第三方合作伙伴来扮演那些不再增加价值的角色，比如效益管理、人力资源、信息中心、旅游服务、保险和股票估价。

虽然商业领袖们很容易明白这些关系的价值，比如支付给专家更低的工资，但是实现起来却比较困难。PCI DSS 和 HIPAA 等都明确规定将严惩入侵以及传输含有敏感信息、金融信息和个人信息的数据。另外，美国具体处理违约通知条例表明，企业应为个人信息以及金融信息泄露负责，即使这是由第三方的安全缺陷造成的。出于这些风险考虑，许多金融公司选择将信息保存在公司内部以保证其安全性，但是允许他们的合作伙伴来管理这些数据。这就导致身份管理联盟技术的兴起，OASIS 的安全声明标记语言（SAML）就是其中的一种。然而，就像 90 年代的公钥基础设施（PKI）的发展一样，采用"信任通道"的安全策略来管理企业与其合作伙伴的合作仍然滞后于商业发展的需要。

身份管理联盟

身份管理联盟发展滞后是有一些原因的。其中最主要的原因是金融公司与其合作伙伴之间缺乏如何进行"信任通道"的合同规范。没有适当的合同规范，公司就没有办法确定采用第三方之后给他们带来的风险，如果第三方违反条例后他们的责任会在多大程度上得到缓解。

另一个主要问题是，在身份管理联盟中，一个身份管理服务供应商要向多家合作伙伴提供信息身份管理服务。而运作这么多的身份管理要经过很多版本的多项条约，管理的复杂性不言而喻，所以很少有公司愿意成为身份管理服务供应商。

而信任关系信息传输过程中的主要技术也是造成管理复杂性的一部分原因。数据联合技术的采用使得"安全声明"的传输得以完成。数据联合技术包括：安全声明标记语言和自由联盟（Liberty Alliance，一个致力于解决数字身份问题的业界联盟）的身份认证联盟框架（ID-FF），这两者都是切实可行的解决方案。现在已有三个版本的安全声明标记语言被金融产业采用，它们分别是：V1.0、V1.1 和 V2.0；还有两个版本的 ID-FF 被采用：V1.1 和 V1.2。

虽然它们都是可行的，但是互相之间却不兼容。这就需要公司支持多种技术，甚至所有的技术。

最后，很难保证第三方能通过正确的授权进行系统查看和管理金融公司的信息。

(作者：Randall Gamby 译者：Sean 来源：TechTarget 中国)

身份管理联盟最佳实践（下）

身份认证联盟的关键考虑因素

怎么才能使身份认证管理的效率提高呢？可以根据以下这些步骤：

- 了解商业内容 ——在公司寻找合作伙伴之前必须了解外包公司的职能，并将其分类，战略性的运作必须排除在外包考虑之外。
- 了解工作流程——一个寻找外部合作伙伴的公司，必须了解其合作伙伴进入和离开公司业务的关键点。公司还必须知道数据是会继续在自己的限制范围之内还是会被合作伙伴带走。要反映新的商业运作流程，就必须对现有的工序和程序进行适当修改。
- 确定信息敏感度——公司必须清楚各个职能中包含的信息种类，其中是否包含敏感信息、金融信息或者个人信息。公司还需要清楚有无与这些信息相关的法律法规。公司必须与可能的合作伙伴共同决定接触这些信息的人员是否需要其他的背景，在被授权接触这些信息之前是否需要其他的确认。最后，公司必须决定这些信息有没有价值，如果出现信息丢失或者泄露时，有没有必要采取补救措施。
- 确定准入合作方的资源要求——一旦公司知道每个职能包含怎样的信息，就必须制定合作方进行职能管理的权限：身份管理联盟技术的行政身份，管理联盟关系的管理身份，使用联盟服务的应用服务和项目的系统准入以及使用联盟技术的终端用户的权限。
- 定义安全声明，确保信息安全——在得知了信息敏感性和访问需求后，金融公司就有能力定义合同义务、安全控制和通信需要，以确保合作伙伴的授权用户可以安全地就与业务功能有关的信息进行交流。这些都应传达给合作伙伴公司征求同意。
- 确定安全声明协议需要沟通渠道的支持——在这一点上，公司应该与它的合作伙伴确定合适的协议——安全声明标记语言、自由身份认证联合框架，或两者都有——并且各个版本都将要予以支持。如有可能，该协议的最新版本应该是用来提供给请求者尽可能多的信息量，他们将在与金融公司的信息交互发挥作用。

这一点会很有争论。金融公司理所当然想支持一个最小的协议以减少他们的支持成本，而合作伙伴想支持他们所使用的标准。另外还存在合作伙伴不具备任何联合能力的风险。虽然不

是最佳选择，但其他方法可能需要授权，如同步登陆/密码信息，但这应该被视为一种短期减损控制。在任何情况下，只要是同意的就应该纳入到合同中和未来的迁移，即从用户名/密码到安全声明标记语言在未来的两年应该与将会蒙受的损失和转换的时间表一起归档。

- 定义审计水平和报告要求——金融公司与它的合作伙伴共同确定审计和报告的水平是十分必要的，这可以确保合同条款和条件的规定。
- 定义如何管理沟通渠道——如果金融组织不希望提供身份服务，它必须把这一责任推给合伙人或寻求国际知名公司，如平安身份认证公司，它为公司及其合作伙伴提供第三方联合经营服务。利用第三方企业的明显优势是它可以提供联系到一家公司的所有合作伙伴，并且在必要的时候进行协议转换，而该公司不用承担正在进行的联系和管理费用。缺点是，公司必须为使用该合作伙伴的服务做额外的预算。
- 制定计划——在达成一项合作伙伴如何接触金融公司以及它会履行什么职能的协议后，该公司应建立一个执行计划，包括时间表、所需资源、结构变化、流程定义、筹资模式和商业抗辩理由。这些在执行之前都应该经过专门的渠道正式批准。

在理解了与第三方合作如何有利于公司，以及理解了围绕使用他们的服务而制定的周密计划之后，金融公司可以降低为他们的股东、客户和合作伙伴提供优化服务的风险。虽然通讯部分只在一个方面起作用，但如果没有它，你的系统将继续在真空中工作，而其他金融行业将把你的公司远远抛在后面。

（作者：Randall Gamby 译者：Sean 来源：TechTarget 中国）

鉴定网银用户身份的最佳程序

基于无线传输和互联网的技术（比如移动银行、远程存取以及网上付款等）事实上已经成为 21 世纪银行关系（banking relationship）平台的标准：你可以在世界上的任何地方进行存/取款活动。传统的客户关系已经被新技术所替代，这让客户关系完全超出了物理银行（physical bank）的范围，而且没有回头路。这些新技术令人激动、更加有效，而且功能更强大，然而要通过跟这些技术相关的客户身份证明程序（CIP）来识别你的客户（KYC）却变得越来越复杂了。

KYC 规则遵从以及 CIP

KYC 规则遵从的本质就是在企业中确立一个有效的客户识别程序，以此遵守反洗钱法规。一个客户可以是一个人、一个公司、合作伙伴、信托机构或者一个实体（estate），所以要使用合适的文档或者通过其他非文档形式的方法来验证或者识别他们。KYC 就是要知道那些客户是谁以及他们跟一个金融机构之间的关系中包括哪些业务活动。

新技术跟旧 CIP 规则遵从过程并不一样

确认任何银行关系所需要的典型客户信息，包括名字、出生日期、地址以及税务识别码。下一步就是验证所提供的信息。根据关系类型不同，需要验证的可能是一系列范围很广的文档，从驾照、护照或者纳税申报单一直到公司文档或者水电费账单，等等。

问题是新技术以及相应的产品难以适用原来的或者传统的遵从程序。不管产品的情况是什么，一个机构都应该牢记客户以及他们的文档仍然是需要核实的。如果他们只是敲击了回车键并发送给你某些信息，这并不意味着真的就是他们本人。

举个例子，一个新客户可能会通过使用互联网的存款单活动（Certificates of Deposits (CD's) campaign）来访问你的机构。互联网有助于你超越地理位置的物理限制来开拓新市场，有助于企业的竞争，但是你怎么来验证这个客户呢？新技术以及新市场需要新方法来做这些事情，因此为了评估和减轻新操作环境带来的风险，人们需要采用新的步骤。

CIP 规则遵从的非文档（Non-documentary）方法

如果你没有原始的识别验证文档，那么你该怎么办呢？如果检查时无法获得原始文档，而客户又不在营业大厅或无法亲自到银行来，企业可以采用几种非文档技术来满足检查人员的需求，对他们而言也是可以接受的。

需要指出的是，企业选择任何一种方法来代替传统的验证方法都应该进行彻头彻尾的记录，还应该对风险评估进行升级，而且在实施之前这些程序都应该由高级管理人员以及董事会批准。非传统的方法依旧需要传统的审批过程。

- 非文档方法包括：

1. 通过其他的银行关系参考（存款或者贷款业务）对客户进行验证
2. 接收文档的扫描副本，但是随后通过查询公共记录来验证该机构，比如：
    a) 公司章程
    b) 良好的信誉证书
    c) UCC-1 文件
3. 访问信用报告信息并把它跟网上应用程序提供的信用报告信息相比较。建议包括：
    a) 目前的信用关系
    b) b.目前以及以前的地址
    c) c.现任以及前任的雇主
4. 获得雇主信息以及工资表建议（用收到的文件代替支票，以此当做直接存款的提示）

我的观点是，如果你仔细考虑了各个选项，并制定出一个依靠信用资源的验证方法，那么你仍然可以在网络环境中核实客户、公司或者业务是否存在。关键是确定所需要的信息，然后使用验证步骤来达到接收并检察原始文件相同的效果。

KYC 规则遵从的后续监视

银行环境全面电子化并不是一件坏事。相反，它给一个企业带来了全新的可能性。此外，当考虑或者使用互联网的时候，KYC 规则遵从并不太困难，但是会有很大的不同。当创建一个虚拟关系的时候，你还需要开发监视这个关系的方法。开始设计在线产品时，你的设计还应该包括一个跟此技术相一致的监视部件。案例证明：在某起事件发生后，月终的批处理报告并不足以应对那些当日实时的业务。如果那时你才意识到出了问题，已为时太晚了。

充分考虑新技术的各种影响是你保护企业所能做的最好的事情，同时这样做还能够创建一个成功的 CIP 规则遵从框架，从而满足反洗钱法的规定。

（作者：Dan M. Fisher 译者：Sean 来源：TechTarget 中国）

网上银行安全的评估工具

最近，根据公开的报告，五名窃贼被指控从美国加州卡森市的银行账户中偷窃了 45 万美元。 2007 年，他们成功地在该市财政局长的笔记本电脑中植入了变种的 Talex 银行木马，并截获了数字证书和账户信息。遗憾的是，这并不是一起孤立事件。许多小企业和市政当局的电脑都正在被复杂的以银行账户和银行数字证书为目标的恶意软件感染，如 Zeus、Clampi 和 Silon 等木马。此类银行木马大多数是通过修改网页、插入新的对话框、篡改 Cookie 等手段感染用户的浏览器，比传统的中间人（man-in-the-middle）攻击更有威胁。为了应对这些威胁，许多商业和自由软件应运而生，确保用户能方便安全地连接到网上银行。让我们来探讨一下这些网上银行安全工具以及它们各自的优缺点。

位于纽约的 Trusteer 公司的 Rapport 软件可能是如今最出名的商业网上银行安全产品。金融机构在其网站上安装 Rapport 系统之后，用户可以下载并安装客户端软件，以此来保护浏览器和通过浏览器与金融网站进行的交互。该软件可在 Windows 和 Mac 系统下运行，通过监测应用程序编程接口（API）来确定是否有其他程序正在试图监控或操纵它们。例如，在 Windows 系统中，WinInet API 被用来建立 SSL 通信，它经常会遭到银行类恶意软件的访问和修改。通过防止恶意软件劫持和修改浏览器，Rapport 能防范 Zeus 等木马的最新的浏览器中间人（man-in-the-browser）攻击。此外，Rapport 是经常更新的，像杀毒软件一样，这使其能够帮助用户抵御恶意软件的最新变种。

使用像 Rapport 这样的软件（或者像英国 Prevx 公司提供的类似的网上银行安全方案 SafeOnline）的好处在于它们能够提供针对浏览器和终端的基本保护，最小化针对大多数终端的冲击，以及检测银行网站的负载能力。然而，许多银行并不想让这个软件成为强制性的，因为用户会觉得安全措施是被"强加"给他们的。此外，该软件需要安装代理才能使用，并可能需要本地管理员访问权限和浏览器的特权用户，以网络安全的实际角度来看这两者都是不可取的。攻击者也不会就此而止步——Zeus 木马和其他恶意软件的新版本已能够检测甚至阻止 Rapport 的某些版本以及其他一些保护性软件的运行。最后，某些保护软件还可能与其他程序或解决方案发生冲突，例如流行的共享软件 Sandboxie。

Sandboixe 或其他类似的软件系统，会在系统中创建一个保护性的独立空间（称为"沙箱"，sandbox）供所有指定的程序运行。如果浏览器是一个孤立的程序，那么即使恶意软件被执行了，沙箱也能够防止其感染系统的其余部分。有一些系统用硬件来实现同样的功能，即

运行自带的浏览工具和环境的 USB 设备。以加密便携硬盘而著名的 IronKey 公司，现在推出一款叫做"可信虚拟计算"的产品。该产品提供了直接在 USB 硬盘运行的虚拟操作系统和浏览器。除了独立的操作系统和浏览器外，该设备还具有内置的反恶意软件扫描和多参数 RSA 认证功能，以及在线更新以防范最新的威胁。这个工具的优点在于不必在主机上安装额外的软件，同时又能在访问金融网站期间更加有效的隔离浏览环境和主机系统。

另一种基于硬件的解决方案是 IBM 公司的区域信任信息通道（Zone Trusted Information Channel，ZTIC），它首先会与预配置的银行网站建立一个安全（SSL/TLS）会话，然后允许主机系统通过浏览器以类似于银行代理的方式进行连接。当用户访问银行网站并输入信息时，它将显示在 USB 设备的 LED 屏上，同时只有在用户手动点击设备上的按钮时，该信息才会传递给银行。这可以阻止浏览器中间人（man-in-the-browser）攻击者任意修改数据或站点信息而不被察觉的现象。不幸的是，这些基于硬件的解决方案需要用户在物理键盘上输入信息，而这很容易被按键记录功能所截获。

一个简单且免费的网银安全的选择是使用一个装有相关操作系统的可引导的 CD/DVD 光盘，只需运行一个被加载到内存中的只读操作系统即可。类似的操作系统发行版本有许多（通常包括 Knoppix、SLAX 和 Webconverger），这些光盘有时被称为"Live CD"。利用 Live CD 的好处是浏览环境与主机操作系统完全隔离，因为用户需要手动从 CD/DVD 启动并引导到只读环境。该操作环境在与银行进行会话期间不会被修改，会话完成后也没有任何信息保存，以防止丢失或者泄露机密数据。这种方案的缺点是需要从光盘启动到只读操作环境中，当然也就需要对用户进行培训。

随着越来越多的银行客户遭遇到由恶意软件所造成的金融诈骗，人们对这种网银安全工具的兴趣无疑会继续增加。这些解决方案各自都有明确的优点和缺点——从"软件安装"到"它们是否能真正隔离浏览环境与操作系统"。但不管怎样，成本始终是银行和终端客户在选择时应考虑的因素之一。

（作者：Dave Shackleford 译者：Sean 来源：TechTarget 中国）

如何检测和预防内部欺诈？

随着整个银行界正在经历复苏的巨大阵痛，欺诈的出现也只是一件不足为奇的事。其中，最令人不安的是职业欺诈（occupational fraud），也常常称作内部欺诈（insider fraud）。认证欺诈检查员协会（Association of Certified Fraud Examiners）将此定义为："通过故意滥用或误用组织的资源或资产，利用个人职务之便为自己谋取利益的行为。"

当欺诈发生时，组织越是自动化，经理和主管就越难直观地识别出欺诈活动。细微的按键就可能引起一次金融机构资金欺诈活动。虽然有软件程序在监测和分析交易数据，以识别那些电子形式的活动，提高欺诈嫌疑，但是需要为软件支付的费用让很多金融机构望尘莫及。

那么，如果在没有技术可以根据分析员工的活动来告诉银行和其它金融机构应该监控哪些事情和哪些人的情况下，这些金融机构可以做些什么工作来发现内部诈骗呢？这一切都可以求助于老式的人事管理：了解你的员工，并认识到员工在"惹上麻烦"和处于欺诈风险时可以起到提示作用的个人行为和情况的变化。

大多数人会情不自禁地在行为上反应出他们的心理和情绪。当人们正在做他们知道是错的事情，或者被迫做他们不愿意做的事情，或者正在做违反道德观念让其内疚的事情时，在行动中可能被抓住的恐惧将使他们的行为出现明显的变化。

然而，经理不应该不假思索地就断定某一特定行为是内部欺诈的征兆。有很多个人情况也可能导致这些行为，但并不意味着跟欺诈相关。并不是每个面临身体或心理健康、家庭或财政问题的人都存在欺诈行为。大多数金融机构有帮助员工解决严重个人问题的方案，但不是所有员工都知道这些方案的存在，而只有那些精明的经理或主管才能让员工的生活水平与以往相比改善很多。

但是，接下来将要谈到的行为和情况也可以看作员工不恰当地使用公司资源的迹象。

情绪性行为的变化

工作引起的愤怒：在目前这种艰难的经济时期，很多人失去了工作，个人时间也减少了，在相同或者更少的工资条件下不得不去做更多的工作，甚至没有福利。加上其他工作相关的问题，比如晋升受阻、因为销售业绩被重新分配到较低工资等级、公司合并或重组，或看到朋友

失去工作，我们发现这些情况都可能使员工有理由采取行动报复雇主。最初失望引起的愤怒是可以理解的，而在之后的工作中仍然带着愤怒的情绪则是一个危险的征兆。

个性的改变：每个人都有自己的个性。有些人天生活泼和外向，有些人害羞。每个人都是独特的，他们对"正常行为"的定义各不相同。当一个人的个性出现明显的变化时（例如，活跃的人变得安静而忧郁，稳重的人突然变得招摇或轻浮），则有理由引起管理者的高度重视。

使注意力偏转：最好的防守就是进攻。有些人不断地干扰他人的注意力，其目的常常只是使别人不去关注他们的不正当行为。

生活方式的改变

消费远大于收入：购买捷豹汽车、金光闪闪的高价首饰、衣柜里的衣服突然更新换代，或者为孩子购买昂贵玩具，这些都不是年薪 30,000 美元的员工所能承受的，同时也暗示着员工具有"其他的收入来源"。当然，这些钱也可能是由于结婚而获得的财富，或者是继承亲戚的遗产，甚至是走好运中了彩票，不过这些钱财的来源依然值得经理去调查一下。

存在经济问题的迹象：有许多迹象表明，职员确实受到了外界的诱惑，为了额外的收入去做那些自己不应该去做的事。这些迹象包括：生活方式突然变得很简朴；上班期间接到对自己干扰很大的电话；时常要求加薪；从原来的居住地搬到花销较低的居住区；经常要求加班。

嗜好：我们都知道有些嗜好需要很多的钱才能得到满足：酗酒、毒品、赌博和嫖娼。还有一些嗜好在普通人中很常见，也有可能和欺诈活动联系起来，比如购买衣服、收藏品、艺术品以及汽车等。这些嗜好都能让人变得疯狂，为了钱财铤而走险。

虐待的迹象

身体上的虐待：工作时，职员受伤或者是肢体受到损害，而员工对其受伤的原因却解释得不合逻辑；为了员工自身的安全着想，这些人应该及时得到经理的关注。然而，有些员工是被迫伤害自己的身体以进行欺诈，从而给家里带来更多的金钱；也有一些员工用自残得来的钱去让自己或自己的子女过得更好。

情感上的虐待：与身体上的虐待类似，语言上的虐待也能给人带来伤害，不过受伤之处是人的心灵。在情感上进行自我虐待的职员可能会做出以下事情：不愿参加工作之外的活动（例如，和同事共进午餐、工作之余的酒会、节日聚会），理由是"我的配偶/男朋友/女朋友不希望我去"；工作期间，经常接到同事的电话，这让他们非常紧张；表现出缺乏自信；不和其他职员发展友情。这种情感上的自我虐待和身体上的虐待一样，都是真实存在的，并且很容易让人去做欺诈的事情。

秘密行为

对于有些秘密的行为，监管人员应该有所注意，因为这些行为有可能是内部人员进行欺诈活动的征兆。比如，内部职员会做以下的事情：

- 时常注意"老板"在哪里。
- 不时地抬头，看看有没有人注视自己。
- 似乎在抽屉、钱包、兜里或其他地方藏着什么东西。
- 出现在与自己本职工作不符的地点。
- 把拥有存储功能的个人物品（例如，闪盘、照相机、照相手机或者是苹果音乐播放器）带到工作环境中来。
- 在复印机或传真机上花费大量不必要的时间。
- 对自己的工作过分保密，不愿别人参与。

你需要记住的是，虽然有上述行为的职员不一定就在进行欺诈活动，但他们却具有从事这种活动的可能性。聪明的经理会采取预防措施，比如安排内部审计人员或者经过充分培训的调查员去悄悄审查职员最近所从事的活动，从而确认职员是否真的进行了欺诈活动。

(作者：Jodi Pratt　译者：Sean　来源：TechTarget 中国)

金融服务领域数据分类的最佳实践

大多数信息安全从业人员都会同意这样的观点，即数据的重要性是各不相同的。换句话说，某些数据与其他数据相比更为敏感，更应该受到严格的保护。数据有很多不同的类型，其相应的敏感性程度也大不相同。金融机构内的安全团队应当如何去保护这些各不相同的数据类型呢？这就是数据分类（data classification）所涉及的领域，即每种数据类型都有自己特定的"标签"，而这些标签与基本的规则关联紧密，比如访问控制、加密、业务流程和数据处理等规则。

许多数据分类的最佳实践和计划都源自经典的安全和风险管理框架，例如 ISO 27001 和 COBIT。在很多情况下，ISO 27001 被用来开发与 Gramm-Leach-Bliley Act （GLBA，金融服务现代化法案）相吻合的控制。该标准的 A.7.2.1 节规定了数据分类指导方针应该如何进行创建和维护。FFIEC（美国联邦机构检查委员会）在颁布的信息安全 IT 考试手册中特别声明了数据分类的必要性。手册将数据分类与"保护设定文件（protection profiles）"相联系，描述了应该采取何种措施去保护特定的数据类型不受曝光和丢失的危害。

既然数据分类如此重要，金融机构应该如何进行这项过程呢？下面是一些在数据分类的最佳实践中，所有机构都应该遵循的关键步骤。

1. 规定哪些数据是重要的，知道这些数据如何储存和转移。对金融机构而言，这一步 骤主要由以下方面的财务数据构成：客户（银行账户和个人信息）、公司财务记录（收入信息、销售数据）、与金融系统有关的知识产权，以及与认证和访问控制信息有关的数据。然后，与个体业务单元合作，评估应用结构和网络图，进而确定在何处存储数据，如何存储，以及数据在环境中如何移动。要确信已经将所有的合伙人和互联网都考虑到了。

2. 规定数据分类类别和标签。这一步骤应该与业务单位共同开展，把重点放在金融或其它具有敏感性的数据类型上。首先，依据数据的保密性和危急层次对分类类别进行定义。举个例子，针对保密性进行的分类可以包括：公开（任何人都可以访问）、受限访问（只有特定的群体可以访问）、保密（受规则和法律授权的控制）。金融服务团队建议，应该将这些标签与危险程度结合起来：

    a) 低：数据曝光和不正确使用不会造成财产损失和法律责任。

b) 中：数据曝光会造成有限程度的法律责任、客户信任的丧失和财产损失。

c) 高：数据曝光会导致重大的法律责任、客户信任的丧失和财产损失。

d) 很高：数据曝光和误用能带来灾难性的罚款、法律责任、客户信任的丧失和财产损失。

3. 规定可接受性使用。数据的可接受性使用应该将内部和外部的规则遵从要求作为基础（包括各州颁布的数据泄露法），还要考虑谁会使用这些数据以及如何使用。在大多数情况下，数据的创建者会被指定为"所有者"，而创建数据的个人或者团体应该具有对数据的使用权限。例如，客户的银行数据只能有客户本人（数据"所有者"）和交易处理员工才能使用。

4. 升级政策要反映出数据分类。确定了政策中已包含数据分类类型和规则遵从的影响，金融机构就可以将数据分类类型与安全意识、事件响应以及其他的危机处理方案措施结合起来。

5. 建立一个维护过程。一个标准的数据生命周期包括以下阶段：创建、存储、使用、修改、保留和存档，以及清除。在每一个阶段里，数据的分类和安全都要通过常规的过程来处理。

虽然数据的分类是一项很复杂的过程，但有一些工具可以提供帮助。几家供应商提供了一些具有电子发现功能并结合了存储系统的产品，（如，EMC 公司的 Kazeon 系列产品和 StoredIQ 公司的智能信息平台），它们都能支持大型企业的数据分类工作。

尽管对数据进行分类和追踪不是一件容易的事情，但这些工作是金融服务机构进行数据保护的核心部分。许多规则遵从规定以及安全最佳实践框架都要求必须具备一定程度的数据分类，而且需要将安全工作的努力集中在更为敏感的数据类型上，从而有利于实现操作效果和效率的最优化。根据以最敏感客户和内部数据为基础创建的"保护设定文件"来看，金融机构可以更好的规划和制定自己的预防、检测和响应措施。

（作者：Dave Shackleford 译者：Sean 来源：TechTarget 中国）

如何阻止ATM卡片浏览诈骗

对大多数银行客户来说，ATM（自动取款机）是一个检查账户、取现金的安全场所。但渐渐地，对不警觉客户而言ATM正变成一个诈骗陷阱。例如今年2月在美国波士顿，3人因向美洲银行（Bank of America）和国民银行（Citizens Bank）所属的ATM里植入假冒的读卡器而被警方抓捕。在被逮捕前，他们累计获得的不义之财高达137 000美元。

据专家介绍，把假读卡器植入到ATM里以采集银行卡数据的诈骗手段被称为“卡片浏览（skimming）”，这种诈骗手段在美国以及世界各地都在快速增长。据SecurityCurve咨询公司的创始人Diana Kelley称，对全球的银行和消费者而言，ATM卡片浏览每年导致的损失大约为10亿美元。

Javelin Strategy & Research是一家金融服务分析和咨询机构。该机构四月的一份报告显示，在美国，所有欺诈受害者中有10%的人曾在假冒的ATM上提取过现金，结果23%受害者成为了其他金融机构的客户。Javelin的研究分析师Robert Vamosi表示，在美国，近20%欺诈受害者的PIN（个人识别号）被盗。

先进的ATM卡片浏览设备

诈骗专家表示，虽然过去5年一直存在着卡片浏览问题，但现在这些设备已经变得更加精密和难以察觉了。仅在美国就有超过425000台ATM可以成为罪犯的目标，他们可以在不同地点的各种ATM上试试自己的运气。

FICO（Fair Issac Corp）是一家提供FICO信用评分以及欺诈检测产品和服务的公司，该公司的高级欺诈解决方案总监Michael Urban说，“从制造或者购买的角度来看，ATM卡片浏览设备都比过去更为先进，这也使得用户更难辨别这些设备。罪犯还使用了和ATM制造商相同的油漆和表面加工。”此外，他补充说，“现在许多罪犯通过蓝牙或GMS手机信号来传输所盗窃的数据，而不必回到ATM处去获得存储的数据”。

PG Silva咨询公司的首席咨询师Jerry Silva同意上述的观点，“罪犯是根据ATM的颜色来进行复制的。即使整个外观发生了变化，消费者也很难区分出来”。

SecurityCurve公司的Kelley表示，一款优质的卡片浏览器（skimmer）的价格大概在5000到8000美元之间。现在的许多卡片浏览器都有卡片读取器和重叠的键盘，这使得卡

片数据和 PIN 都可以被获取。另外，罪犯也可以利用一个隐藏的摄影机来窥视消费者所输入的安全密码。咨询师们表示，不管罪犯将目标锁定在哪个地方，他们都更趋向于攻击最常见的 ATM，但实际上所有类型的 ATM 都存在着风险。

银行和 ATM 的销售商正尝试各种方法来阻止卡片浏览，比如将商业广告放在 ATM 上显示以提醒消费者关于卡片浏览的事情、向键盘和读卡器添加倾斜角使得卡片浏览器更难安装，或者添加传感器以检查 ATM 机是否装有其他设备并向银行员工发送警报。另外，还有在物理上起作用的"振动（jitter）"技术，它能使卡片在进入读卡器时发生抖动，从而使得卡片浏览设备更加难以读取卡片的信息。但是，一些专家表示振动技术并不是一个全方位的防护措施。

ATM 卡片浏览保护

除了反卡片浏览技术外，金融机构还可以采取以下措施来保护 ATM 以及客户免受来自卡片浏览器的攻击：

1. 每天对 ATM 进行一次物理检查。Silva 说："最佳的实践是，每当 ATM 周围挤满了人，就进行一次物理检查"。如果卡片浏览器已经安装在你或者你竞争对手的 ATM 上，采取这一措施就显得尤为重要了。FICO 的 Urban 说："你需要增加检查次数，并派人每天外出对 ATM 检查几次，包括下班后和周末。罪犯会考察每一个他们即将下手的地点，如果他们发现这个地点加强了检查，便可能会另选其他的目标。虽然这是一个技术含量比较低的解决方案，但它往往行之有效。"

2. 加强 ATM 外观的标准。Urban 说："ATM 视觉标准的采纳将会使所有 ATM 看起来都应该是一样的。"他同时指出，分行的经理可以在这类 ATM 里面加入一些东西，但其他的 ATM 则没有加入，这样它们看起来显得略为有些不同。他说："一间分行决定在 ATM 上设置一个型录架（brochure holder），另一个分公司则没有安装这样的设置，这将使得 ATM 的外表五花八门。你希望它们的标准尽量趋向一致，这样你就可以判断 ATM 是否装有卡片浏览器了。"

3. 确保 PIN 输入设备符合支付卡产业安全标准委员会（Payment Card Industry Security Standards Council，PCI SSC）的标准，该委员会管理着 PCI 数据安全标准。PCI SSC 还有针对商家的指导方针：《卡片浏览预防：商家的最佳做法》，其中包含了可以帮助商家精确地找到漏洞的自我评价表格。

4. 查找客户账户的异常活动。Urban 说："虽然欺诈检测软件不是万无一失的，但它可以检测出与欺诈交易相关的一些行为。"例如，一个客户总是在本地使用自己的借记卡或信用卡，突然间在巴西做出一次大规模的采购，这时该软件就可以向银行发起提

醒，这可能会延迟交易，直到其合法性得到验证为止。Urban 表示，客户最新的联系信息在迅速核实交易的合法性或停止欺诈行为方面至关重要。银行账户监控也需要经常更新自己的客户数据。

5. 与其他银行的安全人员建立工作关系。Urban 表示，电子安全工作组的深入参与、甚至与本地其他的银行临时合作，都可以在卡片浏览器窃取各自的 ATM 数据时，帮助银行安全管理人员。

Chip 和 PIN 银行卡

卡片浏览问题的最终解决可能要借助于智能卡技术（Chip 和 PIN）。该芯片携带数据但没有磁条，可在世界范围内广泛使用。欧洲各国正在过渡到 Europay、MasterCard 和 Visa (EMV)智能卡规范，该规范需要一个微型芯片和磁条来完成交易。当 EMV 成为欧洲的标准时，一张只带芯片数据的克隆（cloned）卡将被拒绝，这将于 2011 年开始实施。根据 Visa Europe 的调查数据，欧洲的 4000 多家银行和支付服务供应商已经开始发行 2.5 亿张符合 Visa EMV 标准的 Chip 和 PIN 银行卡，并将同时对数百万台读卡器进行升级。

然而，美国在近期内并不会紧跟欧洲的脚步。

Silva 表示，“ATM 欺诈的损失还没有大到让美国银行重新发行银行卡和重新部署取款机的地步。因为银行必须对每台 ATM 更换读卡器、更换每个 POS 设备和软件，以及所有的银行卡，同时还要对消费者进行培训。总之，与欧洲不一样的是，诈骗的损失还没有大到让美国银行去做此类调整。”

（作者：Sue Hildreth　译者：Sean　来源：TechTarget 中国）

数据屏蔽最佳实践的四大要素

保护客户信息是所有金融公司的安身立命之本。客户信息一旦遭到泄漏，不但会对公司声誉造成长期损害，而且还会违反诸如 PCI DSS（支付卡行业数据安全标准）、HIPAA（健康保险流通与责任法案）以及马萨诸塞州最近通过的隐私保护法等法律法规的要求，甚至还可能会使公司陷入诉讼和赔偿纷争。正是由于存在这些风险，所以对于金融公司来说，确保只有获得访问授权的员工才可以使用客户信息比以往任何时候都更加重要。

虽然可以采用加密技术来保护客户信息，但这种防御方法很昂贵，而且还会使客户信息变成无法使用的格式。因此，研究人员提出了一种掩盖客户信息的替代性方法：数据屏蔽（Data Masking）。数据屏蔽不改变信息的格式，使其仍可用于开发和质量测试，同时又可以提供足够有效的信息，以服务公司的客户。那么，当金融公司准备采用数据屏蔽技术时，需要考虑的关键因素是什么呢？下面是数据屏蔽最佳实践的四大要素。

确定数据屏蔽系统的部署范围

考虑采用任何数据保护机制的首要任务，就是弄清并确定数据屏蔽系统的部署范围。数据屏蔽最佳实践要求金融公司明确哪些信息需要保护、哪些员工可以获得访问授权、哪些应用程序可以使用受保护的数据以及这些数据在生产和非生产领域的什么地方驻留。虽然这一要求理论上似乎容易实现，但由于大多数金融公司运营的复杂性和业务范围的广泛性，确定敏感信息、可以使用敏感信息的应用程序和可以接触敏感信息的员工实际上是一项艰巨的任务。

另外，确定一名员工是否可以获得访问客户信息的授权并不仅仅是一个非是即否的问题。对客户服务代表来说，他们可能需要访问客户的部分信息以验证客户身份，但并不必访问客户的全部信息。例如，客户服务代表可能想知道客户社会保障号/税号或者其账单/邮政编码的后 4 位，以确认打电话的人确实是该客户。虽然客户服务代表需要访问这一信息来确认客户身份，但他们并不需要完全访问整个社会保障号或账单邮寄地址。确定将信息掩盖到何种程度同时仍可用于商业目的可能比较困难，而且通常还需要法律/合规性部门参与或审查。

确定要采用的数据屏蔽技术

数据屏蔽最佳实践的第二个要素是，确定采用哪些数据屏蔽功能处理敏感信息。现有的数据屏蔽技术具有多种数据处理功能，但并不是所有的功能都适合保持有效的业务上下文信息。这些功能包括：

- 不确定的随机化（Non-deterministic Randomization）：使用随机生成的、满足各种约束条件的值替换敏感字段，确保数据仍然有效，而不会将数据替换成 2 月 30 日这样的日期。例如，将日期 2009 年 12 月 31 日替换为 2010 年 1 月 5 日。
- 模糊化（Blurring）：为原始值增加一个随机值，例如使用一个不超过原始值 8%的随机值替换储蓄账户值。
- 置空（Nulling）：使用空符号替换敏感字段中的值。例如，将社会保障号 404-30-5698 替换为###-##-5698。
- 变换（Shuffling）：变换敏感字段中的值的位置。例如，将邮政编码 12345 变换为 53142。
- 可重复的屏蔽（Repeatable Masking）：通过生成可重复且唯一的值，保持参照完整性（Referential Integrity）。例如，自始至终都使用 26-3245870 替换社会保障号 24-3478987。
- 替换（Substitution）：使用值替换表随机替换原始值。例如，从一个包含 10 万个姓名的列表中用“Mary Smith”替换“Jane Doe”。
- 特殊规则（Specialized Rules）：这些规则适用于特殊字段，例如社会保险号、信用卡号码、街道地址和电话号码等，这些特殊字段在替换后仍保持结构上的正确性，并可用于工作流与检验和验证。例如，将“100 Wall St., New York, N.Y.”替换为“50 Maple Lane, Newark, N.J.”，其中的每个随机值（门牌号、街道、城市和州）构成一个有效地址，可以通过谷歌地图或在线地图查询服务 MapQuest 等应用查找到。
- 标记化（Tokenization）：标记化是一种特殊的数据屏蔽形式，利用独特的标识符替换敏感数据，使信息可以在以后恢复到原始数据。例如，为灾难恢复目的而存储的数据必须在以后可以恢复，或者在业务运行过程中信息必须通过不可信的域时，标记化非常有用。

考虑参照完整性需求

数据屏蔽最佳实践的第三个要素是企业的参照完整性需求，不过这一点在一开始部署数据屏蔽系统时往往容易被忽略。在企业层面，参照完整性通常要求汇总信息，以满足业务范围和资源共享需求。这意味着，来自同一业务范围应用程序的每种类型的信息都必须使用相同的算法/种子值进行屏蔽。

例如，如果业务范围 A 的应用程序的数据屏蔽系统将客户的出生日期替换为 2010 年 1 月 5 日，则业务范围 B 的应用程序的数据屏蔽系统必须将相同的出生日期输入值也替换为 2010 年 1 月 5 日。利用参考完整性，如果一个企业级应用程序需要访问每个已屏蔽的出生日期，则该应用程序可以关联和操作来自这两个业务范围应用程序的其余数据。如果在最初阶段或者甚至在部署了第二个数据屏蔽工具时，仍没有考虑这种要访问已屏蔽信息的工作流，则企业的数据屏蔽系统将需要进行重大的调整和信息的重新屏蔽，除非该金融公司的各项业务之间几乎不发生交互，而这通常是不可能的。

然而，对许多大型金融企业而言，在整个企业范围内使用单一的数据屏蔽工具一般并不可行。由于地域差异、预算/业务需求、不同的 IT 管理组或者不同的安全/监管要求，每种业务范围可能会需要部署自己的数据屏蔽工具。尽管这种情况不影响一般的数据屏蔽处理，但如果不同的数据屏蔽工具由于某种未知原因而不能同步，则可能会造成工作流难以继续。例如，对一个业务范围应用程序来说，出生日期的随机化可能完全可以接受。但对另一个业务范围应用程序来说，已屏蔽的出生日期必须属于一个该应用程序认为有效的预定义范围（例如超过 21 岁）。

增强数据屏蔽算法的安全性

数据屏蔽最佳实践的第四个要素是，保护数据屏蔽工具使用的种子值或算法的安全性。由于数据屏蔽的基本原则是只允许获得授权的用户访问经授权的信息，所以数据屏蔽工具使用的种子值或算法无疑属于高度敏感的数据。如果有人掌握了数据屏蔽工具使用的可重复的数据屏蔽算法，则他或她可以对大的敏感信息块进行逆向工程。一个数据屏蔽最佳实践是采用职责分离的原则，允许 IT 安全人员决定使用什么数据屏蔽方法和算法，并只能在初始部署阶段访问数据屏蔽工具以设置种子值，在部署完成之后 IT 安全人员则不能再访问数据屏蔽工具。

由于 IT 安全人员无权访问日常运营系统，而 IT 支持人员无权访问数据屏蔽算法，从而实现了严格的"职责分离"控制。但是，如果数据屏蔽工具未提供这种"职责分离"控制功能，则 IT 支持人员必须执行周期性的背景调查，并严密审计系统访问，以确保算法未遭泄漏。

未来的计划

数据屏蔽确实具有诸多优势。如果需要的话，可以修改企业应用程序本身以执行数据屏蔽处理，而不需要一个独立的数据屏蔽工具，因为企业应用程序的主要功能通常也是某种形式的数据处理操作。已屏蔽的信息是可读的，如果屏蔽功能使用得当的话，甚至可以使用"类生产"数据有效地测试产品业务工作流。客户服务应用程序（例如咨询台）也不必再为保护敏感信息而在屏幕上刻意抹去演示级功能，因为已屏蔽的数据本身就可以替应用程序掩盖敏感信息。如

果客户信息在被打印之前已经进行了屏蔽处理，则即使打印操作可以执行，也不必担心是谁在使用打印机。但实施数据屏蔽并不像向现有应用程序中添加一个模块或开发一个专门实现数据屏蔽的系统那样简单。正如任何数据保护机制一样，在屏蔽第一条信息之前，企业需要制定计划、确定体系结构以及对未来业务如何运行的设想。

（作者：Randall Gamby　译者：王勇　来源：TechTarget 中国）